Der Faktor Mensch wird oft vernachlässigt

Cyberangriffe nehmen rasant zu. Auch kleine Firmen sind betroffen. Gegenwehr ist machbar

Von Jürgen Hoffmann

Seit Beginn des Krieges in der Ukraine sehen 60 Prozent der Betriebe zwischen Nordsee und Alpen eine gestiegene Gefahr von Hackerattacken. „Je länger der Krieg in der Ukraine dauert, desto wahrscheinlicher werden Cyberangriffe auf deutsche Unternehmen aus Russland heraus", sagt Jörg Asmussen, Hauptgeschäftsführer des Gesamtverbandes der Deutschen Versicherungswirtschaft, in deren Auftrag Forsa Unternehmen befragt hat. Vor allem kleine und mittlere Betriebe machen sich Sorgen. Zu Recht.

„Schon in der Pandemie ist die Zahl der Cyberangriffe auf Mittelständler gestiegen", hat Dietrich Büchner von Dynabook Europe festgestellt, einer Tochter des Sharp-Konzerns, die auf Mobilcomputing-Lösungen spezialisiert ist. Die Zunahme von Remote Work habe Hackern mehr Einfallstore geöffnet, weil sich hybride Arbeitsumgebungen schwieriger absichern lassen. Laut Bundeskriminalamt verursachen Attacken aus dem Netz im Schnitt einen Schaden von 1,5 Millionen Euro. Der Branchenverband Bitkom schätzt, dass zehn Prozent der Unternehmen durch Cyberkriminalität in ihrer Existenz bedroht sind. Bereits im vergangenen Sommer hatte der Digitalverband alarmiert und den Gesamtschaden für die deutsche Wirtschaft durch Datendiebstahl, Spionage oder Sabotage mit 223 Milliarden Euro pro Jahr beziffert. Das entspricht einer Verdoppelung der Schadenssumme gegenüber 2018 und 2019 (103 Milliarden Euro).

Wie können sich Firmen schützen? Dietrich Büchner empfiehlt moderne „Schutzanzüge" sowohl für die Soft- als auch die Hardware, etwa biometrische Verfahren statt Passwörter. Henning Horst, Vorstand für Forschung und Entwicklung bei der Wiesbadener Cybersecurity-Firma comforte, rät zu IT-Sicherheitslösungen, die auf Tokenisierung basieren: „Tokenisierung funktioniert wie eine Kühlkette in der Logistik, die bei Herstellung, Transport und Lagerung nicht unterbrochen werden darf." Comforte „pseudonymisiert" die Daten, wandelt also Namen, Passwörter oder Kartennummern mittels Algorithmen in Buchstaben- und Zahlenkombination um. „Sobald eine Kartentransaktion von einem Zahlungsdienstleister verarbeitet

wird, werden alle sensitiven Daten mit nicht mehr zu entschlüsselnden Tokens ersetzt", sagt Horst. „Damit kann kein Hacker etwas anfangen." Zu den Pluspunkten von Systemen „made in Germany" gehöre, dass sie keine „Hintertürchen" haben, durch die Militärs oder Geheimdienste die Anwenderfirmen ausspähen können. Deswegen entschieden sich mittlerweile selbst Unternehmen aus den USA und Asien für deutsche IT-Lösungen. Beispiel: das US-Unternehmen Pulse. Der Betreiber eines Transfernetzwerks für Finanzbetriebe lässt seine Daten tokenisieren. Die Implementierung war durch intuitive Benutzerfunktionen einfach. Horst: „Mittelständler erwarten zurecht, dass man ihnen Lösungen anbietet, die einfach einzuführen und zu bedienen sind."

Eine 360-Grad-Betrachtung der IT-Sicherheit hält Lars Ackermann für entscheidend: „Hacker suchen täglich nach neuen Lücken in Unternehmen, um sich damit in ihrer Community zu brüsten oder weil sie auf finanzielle Prämien scharf sind, die einige Firmen ausloben, wenn ihnen ein Cyber-Einbrecher ihre IT-Sicherheitsschwachstellen aufzeigt".

Der Chef der One-Stop-Shop-Technologieberatungsgruppe X1F, zu der sieben Betriebe mit rund 800 Mitarbeitern gehören, weist darauf hin, dass moderne IT-Landschaften nicht mehr aus voneinander getrennten Silos bestehen, sondern weitgehend harmonisiert sind: „Alles ist mit allem vernetzt." So lasse sich selbst über ein Smartphone das beste Sicherheitssystem austricksen und an sensible Daten kommen. Ackermann empfiehlt „ganzheitliche Sicherheitskonzepte", die auf den aktuellen Erkenntnissen zur Beseitigung von Sicherheitslücken mit Hilfe spezieller Software basieren. Der Fachbegriff für diese Methode: Penetration-Testing.

X1F-Chef Ackermann registriert aufgrund der aktuellen weltpolitischen Krisen bei seinen mittelständischen Kunden „eine nochmals höhere Sensibilität für das Thema IT-Sicherheit". Auch deshalb erwarteten Betriebe immer öfter von ihren Dienstleistern international anerkannte Zertifizierungen wie beispielsweise die ISO 27001, die das Einrichten und Betreiben von Informationssicherheitsmanagementsystemen regelt: „Ein solcher Nachweis gehört mittlerweile zur Mindestanforderung an IT-Unternehmen."

Bei Edelrid, Hersteller von Kletter- und Bergsportausrüstung in Isny im Allgäu, wird Sicherheit seit jeher großgeschrieben. Jeder Meter Seil wird vor dem Verkauf unter die Lupe genommen. Auch seine IT-Architektur schützt der Mittelständler mit Argusaugen, seit ein Verschlüsselungstrojaner das 220-Mitarbeiter-Unternehmen vor einigen Jahren lahmgelegt hatte. Dabei spielen Mitarbeiterschulungen eine Hauptrolle. „Der Faktor Mensch wird bei Cybersecurity-Konzepten oft noch vernachlässigt", erklärt Christian Laber, Head of E-Learning Development bei der G DATA CyberDefense, einem Spezialisten für IT-Sicherheitslösungen. Nicht so bei Edelrid. „Wir wollen unsere Mitarbeitenden als Knowhow-Träger vor Social-Engineering-Angriffen schützen", sagt der Sicherheitsbeauftragte Dominik Gätje. Er denkt dabei vor allem an die bekannteste Form: das Phishing von Passwörtern und anderen persönlichen Informationen. Für das Abfischen nutzen Cybergangster oft echt wirkende E-Mails, mit denen Mitarbeiter dazu gebracht werden sollen, auf einen Link zu klicken und auf der ebenfalls gefälschten Zielseite sensible Informationen einzugeben. Um dem einen Riegel vorzuschieben, stellte das Edelrid-Management zunächst das Wissen der Belegschaft mit einer Phishing-Simulation auf die Probe. Dafür verschickten die IT-Spezialisten von G DATA an alle Mitarbeiter potenzielle Phishing-Mails. Man stellte fest, dass viele Kollegen sich reinlegen ließen, falsche Links anklickten oder Dateianhänge leichtfertig öffneten. Und die Mitarbeiter meldeten ihre Fehler nicht - „aus Angst vor Konsequenzen", so Gätje. Jetzt durchlaufen die Mitarbeiter von Edelrid seit Januar Security-Awareness-Trainings der G DATA academy. Jeder Mitarbeiter absolviert acht bis 33 Kurse. Bisher mit Erfolg. Gätje: „Die Trainingsmaßnahmen haben unsere Mitarbeitenden sensibilisiert und dazu geführt, dass sich ihr Sicherheitsbewusstsein signifikant verbessert hat."

E-Learning-Konzepte werden oft mit Geschichten und spielerischen Elemente versehen, um den Lernerfolg zu maximieren. „Eine gute Geschichte sorgt beim Zuhörer für positive Emotionen, ein klar vorgegebenes Ziel schafft hohe Motivation während des gesamten Trainings", weiß Gätje. „So bleibt beim Teilnehmer mehr hängen." Und wenn Mitarbeiter verstehen, wie Cyberkriminelle agieren, bilden sie eine „Human-Firewall", die verhindert, dass Angreifer ins Unternehmensnetzwerk gelangen.